

Authority E.O. 13526
 By SP8 NARA Date 10/4/11

~~TOP SECRET~~

TICOM/I-51

Interrogation Report on

Uffz. HERZFELD, Heintz Wolfgang

and Translation of a Paper he

Wrote on the British War Office Code.

The attached document consists of:-

- (a) Interrogation Report of Uffz. Heintz Wolfgang Herzfeld of OKH In 7/VI, forwarded by Director, S.I.D. ETOUSA under reference ETSIG-I/ale/fhc dated 23rd June 1945.
- (b) Complete translation of a paper written by Herzfeld on the breaking of the British War Office Code.

Further papers by Herzfeld on Mihailovic and Tito ciphers will be published as TICOM/I-52.

TICOM

1st August 1945

No. of Pages 27DISTRIBUTION

British
 Director
 D.D.3
 D.D.4
 D.D.(N.S.)
 D.D.(M.W.)
 D.D.(A.S.)
 A.D.(C.C.R.)(2)
 Lt.Col.Leathem

U.S.
 OP 20-G (2)(via Lt.Pendergrass)
 G-2 (via Lt.Col.Hilles)
 S.S.A.(2)(via Major Seaman)
 Director,S.I.D.ETOUSA (via
 Lt.Col.Johnson)

TICOM

Chairman
 S.A.C.(2)
 Cdr. Bacon
 Cdr. MacKenzie
 Cdr. Tandy
Lt. Col. Johnson
 Lt. Cdr. Manson
 Major Seaman
 Lt. Eachus
 Lt. Vance
 Capt. Cowan
 Lt. Fehl
 Ticom Files (2)

Additional
 Major Morgan
 S.A.C. (2 extra) for: D.D.(Y)
 Signals 6, War Office

Declassified by D. Janosek,
 Deputy Associate Director for Policy and Records
 on 12/7/2010 and by dy

Do NOT Destroy Reurn to the
 NSA Technical Library when no longer needed
 5-4551
 T-Comm No. 2

S-6-39-3

DECLASSIFIED

Authority

E.O. 13526

By

NARA Date 10/4/11

~~TOP SECRET~~

2.

J-51

Interrogation Report of

Uffz. HEINTZ WOLFGANG HERZFELD

I. Personal Data:

Prisoner was born in Berlin, 14 Dec 1914, son of a patent lawyer of Jewish descent. He went to school in Frankfort-am-Main from 1922 to 1930 and then in Berlin where he was graduated in 1933. To enter the Technische Hochschule in Berlin, the prisoner was forced to join the National Sozialistischer Studentenbund. He resigned in 1934 because membership in the Bund would have led to membership in the Nazi Party which, he claims, he did not desire because of his descent.

He was conscripted in 1935 and served for 16 months with the 3rd Motorized Reconnaissance Battalion at Stahnsdorf. After service he joined the allegedly nonpolitical Ex-serviceman's League and so was permitted to continue his studies. He received an engineering degree in physical chemistry in 1940 and was working on his doctor's degree when drafted.

The prisoner travelled in England in 1934, 1935, 1937 and 1938. His family had hoped to move to England, but their plans were interrupted by the war.

II. Operational Experience:

1. After 14 months in the Army, most of it spent as an English interpreter, the prisoner was transferred, as a cryptanalyst, to the Inspection VII/6 of the Oberkommando des Heeres. He has drawn a diagram of the organization of this section from 1941-1943, reproduced below as Appendix I. P/W's activities may be tabulated as follows:

<u>TIME</u>	<u>WORK</u>
Aug 1941-July 1943	British Branch - British War Office Code (In addition worked on DeGaulle Central African Code and Trans-Jordania Frontier Force Cipher during a stay at Athens, Jan - Sept 1942)
July - Oct 1943	Italian Branch - numerical codes with additives.
Oct 1943-Nov 1944	Balkan Branch - Tito and Mihailovich traffic
Dec 1944-Jan 1945	American traffic - Slidex
Jan 1945-Mar 1945	Hospitalized
Apr 2, 1945	Taken prisoner

The work after Nov 1944 was done in an R.I. Company. The shift from headquarters was a repercussion of the attempted assassination of Hitler in which a number of headquarter officers had been involved.

2. The prisoner has written out three reports explaining the methods of breaking he employed. These reports are appended. Their contents may be summarized as follows:

a) British War Office Code:

1. Type of code: Numerical, four-figure groups enciphered by means of a subtractor. The subtractor was a Reciphering Table with starting points indicated by five letter groups. Signatures and addresses were concealed in body of text. The Code was fixed and the subtractor changed no more often than every fortnight. The Code book had been captured (at Dunkirk and in Norway).

2. Cryptanalysis: Several messages with same indicator were superimposed. At any given point, since the subtractor was the same, the difference in cipher text was an index to difference in code

Declassified by D. Janosek,
Deputy Associate Director for Policy and Records
on 12/7/2010 and by sp

TOP SECRET

3.

groups. By starting at a point presumed to contain the signature in one message and by comparing the obtained difference with a table of differences of the most frequent code groups, an entry could be made. Extending the entry did not differ essentially from anagramming in depth. Eventually the British introduced "One Time Pads", which defied solution.

b) Mihailović Traffic;

1. Type of traffic: Double transposition using same rectangle and transposition key for both encipherments.

2. Cryptanalysis: There was no general solution. Advantage was taken of stereotyped beginnings and endings containing low frequency letters. Also, for a message of given length, there was little variation in the width of rectangles used. After the correct width had been assumed, the columns could be located approximately and gradually fixed more precisely by extensive use of cribs.

c) Tito Traffic

1. Type of traffic: Numerical monoalphabetic cipher consisting of a one or two digit number substituted for each letter. A short repeating additive sometimes based on a key-word was used for superencipherment.

2. Cryptanalysis: The length of the additive was determined by factoring repeats and the text written in rows of the length of the additive. A frequency count of each column was now made and the digits of the additive apportioned so as to reconcile the maxima of each column. Where this gave no clear-cut results, another column with a clear maximum was chosen for comparison and the proper additive fixed by considering the square of the difference in frequency. Once the additive was removed, the monoalphabet was broken easily.

DECLASSIFIED

Authority E.O. 13526
 By [Signature] NARA Date 10/4/11

J-51

TOP SECRET

4.

APPENDIX I

Approximate Organization of Inspektion 7/6
 Inspektion 7 (Nachrichten) Gruppe 6 (Nachrichten-Aufklaerung)

1941 - 1942

Gruppenleiter: Major Mang*
 Stellv. Gruppenleiter: Reg. rat Bailovic

Referate					
<u>England</u>	<u>U.S.A.</u>	<u>France</u>	<u>Italy</u>	<u>Balkans</u>	<u>Mathematical Analysis</u>
Ob. Insp. Zillman	SdfZ Steinberg	SdfZ Kuehn	Hptm. D.*** Fialla	Reg. rat Bailovic	Sdf K Pietsch

Noteworthy Assistants

Ob. Insp. Liedtke SdfZ Schulz Sdfz Liedtke Wachtm. Schicht Freifrau v. Stael-Holstein	Wachtm. Mueller		Wachtm. Graf.Lt. v. Eszterhazy Denffer Uff. Schlinzigk	Personnel Section: Hptm. - - - Frau Richter
--	--------------------	--	---	--

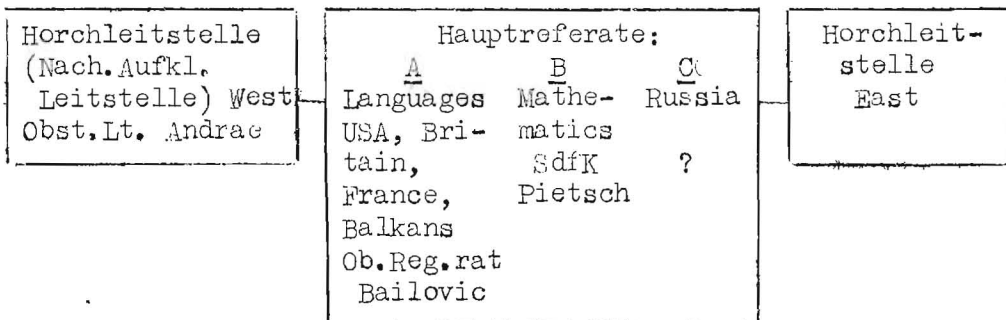
*Major Mettig took over this position at the end of 1942 and held it until July 1943

**Uffz Manaigo subsequently replaced Fialla

1943

During 1943 the full title of the section was changed to "Amtsgruppe Nachrichten, Nachrichten-Aufklaerung". Its general organization was as follows;

In 7/6 (AGNNA) Major Lechner in charge



DECLASSIFIED

Authority E.O. 13526
By [Signature] NARA Date 10/4/11

J.51

TOP SECRET

5.

Organization of the Balkanreferat in 1943-1944

Referatleiter: Ob. reg. rat Bailovic
 Stellv. Ref. ltr.: Sdfz Geiszler (not a cryptanalyst;
 Wachtm. Eszterhazy handled cryptanalytic
 matters for him).

Albania : Uffz. Herzfeld (P/W in question)
Croatia (Army and Ustasa) : Uffz. Schlinzigk (worked also on
 Polish traffic in 1943)
Greece : Wachtm. Kleiner
Hungary : Uffz. Seper
Rumania : Wachtm. Schmidt
Yugoslavia : a) Mihajlovic : Uffz. Glaner
 b) Tito : Uffz. Gradischnigo

DECLASSIFIED
 Authority E.O. 13526
 By [Signature] NARA Date 10/4/11

I-5!

TOP SECRET

6.

DRAFT

INTERROGATION REPORT OF UFFZ. HEINTZ WOLFGANG HERZFELD.

Appendix II

War Office Cypher

The 4-figure code was used in the British Army, as can be proved, from 1940 - 1943 in traffic between Division - Corps - Army.

Two copies of the code were captured:

- 1) In the Norway campaign - April 1940
- 2) Near Dunkirk - beginning of June 1940

It is doubtful whether the British noticed the loss immediately or later on, but it is probable that they did.

Construction of the code:

Part 1 in alphabetical order:

A		6043	
AO		2554	
AA (Anti-aircraft)		0327	(Figures are
Action	ABERDEEN	8953	chosen
Anti		6241	arbitrarily)
Anti-tank	Aden	6770	
Artillery		7012	
Astonish -ed, -ing	Athens	1044	
Attention		9905	
Attorney		2455	

etc.

Part 2 in numerical order:

100 code groups on a page

e.g.	<u>20</u>	00 battery	50 after	
		01 advance	51 much	
		02 reach	52 sergeant	
		03 necessary	53 howitzer	etc.

DECLASSIFIED	
Authority	E.O. 13526
By	SP NARA Date 10/4/11

I-51

TOP SECRET

7.

In October 1941 I had to work on messages from the Middle East. As an example, the British used to encypher some of these messages as follows:-

Encyphering on War Office Cypher.

- A) FROM - FORTRESS - COMMANDER TOBRUK -- TO - 8TH - ARMY - 14TH -
25 OCTOBER - PLEASE - SEND - PLANE - TO - EVACUATE - LT - HARVEY -
Q - M - 212 -
- B) Addressed to - CIPHER OFFICER - 8TH - ARMY - FROM - CIPHER
26 OFFICER - TOBRUK - 16TH - OCTOBER - X - MACHINE - OUT OF -
ACTION -, - SEND - SPECIALIST - FOR - REPAIR - Q - M - / -
305 -
- C) 7TH - ARMoured - DIVISION - TO - 13TH - CORPS - 20 - OCTOBER -
32 SENDING - YOU - ITALIAN - INTERPRETER - CPTN - - - MASSIGLI
--- PLEASE - SEND - ON - TO - GHQ - CAIRO - C - Q - / - 573 -
- D) Addressed to - 13TH - CORPS - 30TH - CORPS - AUSTRALIAN - FORCE
37 - AUSTRALIAN - BASE - FROM - 8TH - ARMY - 20TH - OCTOBER - URGENT
- REQUEST - TO-REPORT - ON - EFFECTS - OF - NEW - ARM - . -
COLONEL - - -NE - AT - HE - RB - Y - R - P - / - 33 -
- E) TO - FORTRESS - COMMANDER - HAIFA - FROM - - MI - LP - AL -
43 20 - OCTOBER - CPTN - - - LO - WT - OF - T - AND - LT --- BE -
CK - IT - T - WILL - ARRIVE - HAIFA - BY - PLANE - TO MORROW -
AT - 15 - 00-HOURS - M - P. 87 - / - 22 - / - 10 -
- F) Addressed to - 8TH - ARMY - VIA - VIA - 13TH - CORPS - FROM -
N - Z - DIVISION - 18TH - OCTOBER - 18 - 00 - GERMANS -
PREPARING TO - RETAKE - - - OM - AR - . - REQUEST - SEND
REINFORCEMENTS - E - O - / - 751 -

The British encypherer first of all wrote in the address, date and serial number in brackets at any arbitrary place in the text. This was intended to avoid stereotyped occurrences of the same message beginnings.

DECLASSIFIED

Authority E.O. 13526

By [signature] NARA Date 10/4/11

8.

TOP SECRET

I-51

Names not appearing in the WOC and other words as well, were spelled out by splitting the word in question into bigrams and encyphering them by a 2-figure substitution table.

For example: MILPAL

00 -	07 G	14 N	21 U
01 A	08 H	15 O	22 V
02 B	09 I	16 P	23 W
03 C	10 J	17 Q	24 X
04 D	11 K	18 R	25 Y
05 E	12 L	19 S	26 Z
06 F	13 M	20 T	27 '

In front of the spelt out word he put in the cypher text the amplifying group:

"spell a word of 6 letters" (as in the case of Milpal)

Spell a word of 2 letters	0002
" " " " 3 "	0003
" " " " 4 "	0004
" " " " 5 "	0005
" " " " 6 "	0006 etc.

So the speller "MILPAL" appeared like this in the cypher text:

0006 1309 1216 0112

Group 2627 "take 2nd interpretation of codeword" meant that of the following code group

9438 = send, -ing, -s

the 2nd meaning i.e. "sending" was to be taken.

Messages encoded on WOC then had the figure text shown in Enclosure 1.

Recyphers. (= Recyphering by a 'recyphering table')

Appendix 2 represents a page out of a recyphering table. It contains 12 lines each having 5 4-figure groups and a 5-letter indicator at the beginning of every line. Of course this can just as easily be a 4-figure or 5-figure group.

DECLASSIFIED

Authority E.O. 13526
By (S) NARA Date 10/4/11

I-51

TOP SECRET

9.

The British encypherer then encyphered, for example, the code text of message A by using the ^{figure} row indicated by the group TODBA. (Enclosure 3).

After this long symbolic subtraction of the code text from the particular portion of the subtractor table, he gets the final cypher text as transmitted by the W/T operator.

Subtractor minus Book group = Cypher Text.

i.e. $S - B = C$.

Assume that an encypherer of the New Zealand Division has a message F to put into cypher at the same time and is, by chance, using the same page of the recyphering table for his subtractor. But he uses as his starting point the indicator DELNI. He then uses the section of the subtractor marked in ink. This is to some extent the same as that used for message A. (Appendix 3).

Decoding.

In decoding the W/T text is subtracted from the recypher and the code text is produced.

Subtractor minus Cypher Text = Book group

$S - C = B$.

The recypher was changed in the Middle East, approximately every 3 weeks, later every 14 days!!

Cryptanalysis. (being in possession of WOC).

Let us assume that there are 5 W/T messages A - E in the material, spread over not too long a period, with one and the same indicator "TODBA". It is presumed that all five messages were recyphered with the same part of the subtractor.

The 5 messages are written down underneath one another (Appendix 4) and it appears that between messages D and E there are 2 "clicks" having the same rhythm, i.e. they are equidistant from the beginning of the message. The appearance of such split repeats is a marked characteristic of recyphers.

TOP SECRET

DECLASSIFIED

Authority

By

NARA

Date

10/4/11

1.

$$B_b - B_g = C_b - C_c$$

$$B_c = B_b - (C_b - C_c) \text{ etc.}$$

By this means are obtained relative values for code groups based on $C_a = 0000$.

It should be observed also that the difference $F_b - F_a$ cannot only derive from code groups $B_b + B_a$ but from any other $B_b + B_a$, e.g.

$$2345 = 3456 - 1111 \text{ and } 4567 = 2222$$

Actually any 4-figure difference can be made in 10,000 different ways. But in the material investigated of course only the difference between frequent code groups will appear predominantly.

Fortunately all these difficulties in establishing a relative code were circumvented by capture of 2 copies of the WOC (in Norway and Dunkirk).

We had a difference table prepared by Hollerith of the code groups which would probably appear most commonly in the addresses. We then proceeded as follows:-

We began with column 18 of the cypher text because we assumed that a frequent address group would be the reason for the "click" in this column. (The "click" in column 24 illustrates that this need not necessarily be the case). We extracted all differences between the cypher texts of messages A to E in this column and obtained these values:-

$$A - B - 4773$$

$$A - C - 3566$$

$$A - DI - 4285$$

$$A - CI$$

$$B - C - 1217$$

$$B - D/E - 2152$$

$$C - D/E - 3369$$

Of each pair of differences (A - B) and (B - A) the smaller difference was always chosen, i.e. that under 5555, as, to save work, only these were included in our difference table.

J-51

DECLASSIFIED

Authority E.O. 13526

By [signature] NARA Date 10/4/11

TOP SECRET

12.

I-51

We now found in our difference table, with others:

$$(A - D) - 4285 = 0749 - 6564 [] - [FROM]$$

$$= 3205 - 9020 [Corps] - [H.Q.]$$

It was necessary to investigate which of the two was more probable. Had 0749, to be put in Message A or was it 6564?

It follows from the equations on Page 14 that:

$$C + B = S$$

If I write in:

in cypher text A 0619 + 6564 = Ba I arrive at 6173 as the subtractor	and in D 4894 + 0749 = Bd and 4:33
---	--

This is obviously wrong as the basic condition was that over Column 18 there should be the same subtractor for messages A and D.

If I write them in the other way round:

In the cypher text A 0619 + 0749 = Ba I get the subtractor 0358 in both cases.	and in D 4894 + 6564 = Bd 0358
---	---

This is therefore correct.

I now calculate the code group in message B in Column 18, in accordance with the formula on page 14.

$$S - C_b = B_b$$

$$0358 - 6946 = 4412$$

and that for message C:-

$$S - C_c = B_c$$

$$0358 - 7153 = 3205$$

In the same way I now write down first the components of the second difference 3205 - 9020 (Corps) - (H.Q.) in messages A and D and obtain:-

In cypher text A 0619 + 3205 Subtractor 3814	and in D 4894 + 9020 3814
---	------------------------------------

Using these I arrive at:

$$B_b = S - C_b = 3814 - 6946 = 7978$$

$$\text{and } B_c = S - C_c = 3814 - 7153 = 6761$$

1-51

There is now a choice between:

(A - D) = 4285

= 0749 - 6564

= 3205 - 9020

Subtractor 0358

3814

B_a = 0749)

B_a = 3205 Corps

B_b = 4412 16th

B_b = 7978 obvious

B_c = 3205 Corps

B_c = 6761 59

B_d = 6564 from

B_d = 9020 HQ

B_e = 6564 from

B_e = 9020 HQ

As a criterion for deciding, I have a look at the intercept date. In most cases this is the same, or the following day, as that contained in the cypher text.

For example, the intercepts are reported to be:-

Message A - 15 October 0450 hours

" B - 16 " 1800 "

" C - 20 " 1530 "

" D - 21 " 0025 "

" E - 20 " 1915 "

" F - 19 " 0120 "

I then notice at once that B_d = 4412 = 16th in the left-hand column tallies with the intercept date of message B. I shall decide, therefore, on subtractor 0358 for column 18 and the values on the left side.

If the group B_b = 16th is actually the date group in message B, then I look for book group 6315 = (Oct) in column 17 or 19. This is then written in as a try-out and the result is:

Column 17

Column 19

C_b 5629

C_b 5754

B + 6315

B + 6315

Subtractor 1934

1069

I now calculate the book groups for column 17:

DECLASSIFIED

Authority E.O. 13526
 By [Signature] NARA Date 10/4/11

TOP SECRET

14.

151

Column 17

Column 19

S - C_a =

S - C =

1934 - 8281 = 3753 Ordnance	1069 - 2124 = 9945 evacuate
1934 - 5629 = 6315 Oct.	1069 - 5754 = 6315 Oct.
1934 - 6726 = 5218 material	1069 - 0093 = 1076 C
1934 - 7727 = 4217 already	1069 - 8047 = 3022 8th
1934 - 4536 = 7408 North	1069 - 1063 = 0006 spell a word of 6 letters

The decision in favour of Column 19 is not difficult as the combinations:

Ordnance)
Oct.	16th
Material	Corps
already	from
North	from

are most improbable, whereas

)	evacuate
16th	Oct.
Corps	C
from	8th
from	spell a word of 6 letters

immediately suggests "from the 8th Army".

I therefore try out "Army" book group 1037 in column 20 in message D and get:

C_d = 4637
 +B = 1037
 Subtractor (Col. 20) 5664

S - C_a = 5664 - 6553 = 9111 Lieutenant
 - 3677 = 2097). (bracket end. Fullstop)
 - 3459 = 2215 Q
 - 4637 = 1037 Army
 - 4365 = 1309 M I (spelling place).

DECLASSIFIED

Authority E.O. 13526
By [signature] NARA Date 10/4/11

I-51

TOP SECRET

15.

So that in 3 columns 18 - 19 - 20 I have:

Message A)	evacuate	Lieutenant
B	16th	Oct.).
C	Corps	C	Q
D	from	8th	Army
E	from	spell 6	M I

letters

By getting M I, I assume immediately that it is MILPAL and thus obtain columns 21 and 22, etc.

I can fill in the text of the message without difficulty as far as the addresses extend, i.e. from Columns 5 to 33 and, as message D ends in a "click", even up to Column 35. The filling in of Columns 1 - 4 would present considerable difficulties if message E did not begin with a speller. I cannot reconstruct the remainder of message E from Column 36 on.

I therefore look through my messages for one which falls under a different indicator, yet at the same time, comes partly under the recypher having TODBA as its indicator.

For this purpose, I must act on the assumption that a message, falling under Columns 20 - 25^{*} of my recypher, if it contains the code group 0000 = . (fullstop) in one of these columns, must contain at this place the cypher text group:

S - B = S - 0000 =

in the column:

i.e. $\frac{20}{1069}$ $\frac{21}{5664}$ $\frac{22}{8549}$ $\frac{23}{7299}$ $\frac{24}{6380}$ or $\frac{25}{7003}$

*
(i.e. $\frac{20}{1069}$ $\frac{21}{5664}$ $\frac{22}{8549}$ $\frac{23}{7299}$ $\frac{24}{6380}$ $\frac{25}{7003}$)

As the starting points of both recyphers can only vary by 5, 10, 20 etc. recypher groups, then the one in messages having a different starting indicator, if they are based on code group 0000 = . "fullstop", can only appear at the 6, 11, 16, 26, 31, 36th place, in other words they must run at intervals of 5.

DECLASSIFIED
 Authority E.O. 13526
 By [Signature] NARA Date 10/4/11

I-51

TOP SECRET

16.

I therefore arrange my Hollerith version of the cypher groups in 5 interval sets or phases:

Phase	I	II	III	IV	V
Contains all	1	2	3	4	5
	6	7	8	9	10
	11	12	13	14	15
	16	17	18	19	20
	21	22	23	24	25
	26	27	28	29	30 etc

cypher groups.

From my tabulation I see that in message F at position 11 (in Phase 1), the group "5664" also occurs. I write in this message under messages A - E (Enclosure 3) so that group 11 falls under the 21st group of these messages (Enclosure 4).

I now subtract the adjacent groups to group 5664 of the cypher text of message F from the recypher obtained from messages A - E and get the following text:

Subtractor	0358	1069	5664	8549	7299	6380	7003
F	9845	1951	<u>5664</u>	0864	9579	3368	6076
Giving:	1513	0118	0000	8785	8720	3022	1037
	?	?	.	(Addressed to 8th Army.		

On looking at positions 1 and 3 of the two groups 1513 and 0118, a speller is suggested, which would be "OMAR". Furthermore, in the case quoted, I know in each case the whole recypher from Column 1 of message F to Column 25.

Without any great difficulty the rest of the recypher from Column 36 to Column 43 can be obtained from message E and message F.

Further Analysis of the WOC System and its Cryptographic Handling.

After the capture of the War Office Cypher in the early summer of 1940, the English Section under Oberinspektor LIEDTKE was successful in establishing

DECLASSIFIED

Authority E.O. 13526

By [signature] NARA Date 10/4/11

TOP SECRET

17.

I-51

the use of the WOC in North Africa in the spring of 1941, in conjunction with Reciphering Table (sic) and 5 letter indicators.

A considerable volume of messages was read, especially during the British Cyrenaica offensive under General Wavell (8th Army) in March. Organisation of the base services and Order of Battle of the Army were recognised or earlier results were confirmed. During late summer Rommels' counter-attack took place, leading to the siege of Tobruk. The besieged fortress was solely dependent on W/T for its signals communications to 8th Army and Cairo. It used almost exclusively the WOC and Reciphering Table, primarily with 5-letter indicator and 5 or 6 subtractor groups per line (i.e. when the messages were tabulated giving phases or intervals of 5 or 6). It then went over to 4-figure indicators. But as it continued to repeat the indicator occupying the first position at the end of the message in clear, it was not difficult for German cryptographers to recognise that the cypher was, in fact, the same one.

To break the address, it was only necessary in most cases to have two messages with the same indicator, and to break the text of the message, 3 - 4 messages.

During the 8th Army's relief attempts in November 1941, which led to the cutting off of Rommel between Tobruk, Bir Omar and Sollum and his famous break-out to the West at Sidi Rezegh, we were able to follow accurately this development and the British units taking part in it.

Our skill suddenly gave out at the middle of December; a few messages could be broken again at the end of December, and then by the middle of January '42, all our attempts at an entry were fruitless.

At this time I was sent to Athens to Nachr. Aufkl. Regt. 4 with a party of 8 cryptanalysts. Rommel was in the Ain-el-Gazala position and was preparing his May offensive. We were quite unable to break into the plentiful traffic bearing 4-figure indicators during the months of February, March and April and so to give Rommel greater intelligence on the rearward organisation of the enemy.

DECLASSIFIED

Authority

By

E.O. 13526

NARA Date 10/4/11

TOP SECRET

18.

J-51

It was only after my return to Berlin in October/November 1942 that I succeeded in doing what could have been done without difficulty in December '41, if only there had been the necessary cooperation in the English Section and a larger number of cryptanalysts had been available

Simultaneously with the use of the WOC with Reciphering Table and 4-figure indicators, the British were using at home for training and practice purposes during the autumn and winter of 1941, the WOC with Reciphering Table and 5-letter indicators. In fact in the whole of the British Isles, they were using only one single Reciphering Table and kept it in force for months until 1/1/42! As against this, in Africa they changed their Reciphering Table every 14 or 21 days.

When I took over the work on the material in October 1942, I retrieved first of all the messages our intercept operators had picked up in the autumn of '41 and which number several hundreds. At that time (end of '41) these were not worked on and classified as practice traffic no-one wanted. A fundamental error! In cryptanalysis absolutely everything produced by the enemy must be worked on and utilised.

I found 5 messages with the same 5-letter indicator and at one place, with our old address group ("from" = 6564) made a break-in which looked approximately like this:

Message A of 6/12	Col. (N) from
B " 15/12	Division
C " 18/12	Canadian
D " 22/12	blank group A
E " 23/12	23rd.

I at once decided that we had here Canadian troops, possibly divisions in U.K. and received confirmation from the Evaluation Section that the 1st, 2nd and 3rd Canadian Divisions were stationed in S.E. England.

I assumed that in Col (N + 1) the word "Division" would occur after "Canadian" and obtained:

DECLASSIFIED
 Authority E.O. 13526
 By [Signature] NARA Date 10/4/11

151

- A from 2nd
- B Division blank group A
- C Canadian Division
- D blank group A is
- E 23rd blank group B

From this I set up message A according to the old WOC. The "blank group A" (a code group of WOC not allotted a meaning), had obviously been given the meaning "from" in messages taken after 15/12. I was able to establish that the British had now filled in, of the approximate 500 blank groups in the WOC:-

- 5 different ones with (
- 5 " " ")
- 5 " " ")
- 5 " " " "from"
- 5 " " " "addressed to"
- 5 " " " . Fullstop
- and 5 " " " - - Dash or hyphen

- in fact just those groups we always used as a starting point when fixing the position of the address.

I also established that as from 1/1/42, a new recyphering table was being used, which ran throughout the year, so that in November '42 there were, for instance, 15 messages all using the indicator HABQY.

From this, it was deduced correctly that the speller-indicating groups and the substitution table for words not included in the WOC had been altered too. e.g.

50 -	57 G	74 N	91 U
51 A	58 H	75 O	92 V
52 B	59 I	76 P	93 W
53 C	70 J	77 Q	94 X
54 D	71 K	78 R	95 Y
55 E	72 L	79 S	96 Z
56 F	73 M	80 T	97 I

DECLASSIFIED

Authority E.O. 13526
By [Signature] NARA Date 10/4/11

20.

TOP SECRET

1-51

By doing this, the objection was avoided of having differences appearing between speller passages in 2 messages on the same recypher, where their 1 and 3 positions lay between 0 and 2 and immediately suggested speller passages.

For example:

Message A	Spell 6	MI	LP	AL
	0006	1309	1216	0112
	Spell 5	DE	RN	A-
	0005	0405	1814	0100
<hr/>				
Difference	0001	1904	0402	0012
	- -	- -	- -	- -

The difference remains constant even when recyphering is done with the same subtractor table; all these discoveries could have been made in December or January '42 if work had gone on uninterruptedly on U.K. traffic and would have made possible the further exploitation of WOC traffic in North Africa.

Meanwhile, the turn in the tide in North Africa had occurred at El Alamein in October '42 and in November the 1st U.S. Army landed in Morocco and Algeria. There was a little WOC traffic and we also set 3 messages with the same indicator (5-letter). However volume was too small to enable successful exploitation.

From December '42 until March '43 the British switched over to the use of 4-figure indicators which were recyphered. For this they used a recypher derived from the groups contained on the last page of their Recyphering Table. Let us assume Enclosure 2 represents the last page. The British numbered the recypher groups on this page 01, 02, etc. If the indicator 7483 had to be recyphered, they chose, for example, the 23rd group 9782 as the indicator recypher and obtained:

$$\begin{array}{r} 7483 \\ + 9782 \\ \hline 6165 \end{array}$$

6165 as the recyphered indicator

DECLASSIFIED

Authority E.O. 13526
By [signature] NARA Date 10/4/11

T 51

TOP SECRET

They disguised the "23" as a recypher reference by using a group having a letter first and at the second and 5 places an arbitrarily chosen figure, e.g.:

G5234

The WT message then began:--

G5234 6165 ... 4-figure text ... 6165 G5234.

Dealing with such an indicator recypher presented no difficulty with the plentiful supply of practice traffic originating in home territory.

Hollerith tabulation gave the following picture with 3 messages:

	Indicator						
A) G	<u>5234</u>	<u>6165</u>	7843	<u>2195</u>	<u>2873</u>	9561	<u>7833</u>
B) B	2651	2117	0514	<u>2195</u>	<u>2873</u>	<u>6299</u>	<u>7833</u>
C) P	<u>8236</u>	<u>6165</u>	9192	4893	<u>2873</u>	<u>6299</u>	<u>7833</u>

Obviously A, B and C were recyphered with the same subtractor and as A) and C) show the same recyphered indicator group, then only the 23 in message No. 1 can be the reference.

We now assumed an arbitrary recypher figure of 1111 for the reference figure 23 and subtracted it from 6165. We thus obtained then the relative indicator group

$$\begin{array}{r} 6165 \\ - 1111 \\ \hline 5054 \end{array}$$

Then, as the group "5054" must also be contained in the recyphered indicator "2117" in message B, we get:

$$\begin{array}{r} 2117 \\ - 5054 \\ \hline \end{array}$$

7163 - the relative recypher for reference No. 65

(from B 2651)

From further matched-up pairs of messages, (matched by reason of "clicks"), we finally compiled a complete "Relative Recypher Table" by using which we could eliminate the indicator recypher without difficulty and could establish which messages had the same (relative) indicator.

~~TOP SECRET~~

DECLASSIFIED	
Authority	E.O. 13526
By	SP8 NARA Date 10/4/11

11.

J 51

$$B_b - B_g = C_b - C_c$$

$$B_c = B_b - (C_b - C_c) \text{ etc.}$$

By this means are obtained relative values for code groups based on $C_a = 0000$.

It should be observed also that the difference $F_b - F_a$ cannot only derive from code groups $B_b + B_a$ but from any other $B_b + B_a$, e.g.

$$2345 = 3456 - 1111 \text{ and } 4567 - 2222$$

Actually any 4-figure difference can be made in 10,000 different ways. But in the material investigated of course only the difference between frequent code groups will appear predominantly.

Fortunately all these difficulties in establishing a relative code were circumvented by capture of 2 copies of the WOC (in Norway and Dunkirk).

We had a difference table prepared by Hollerith of the code groups which would probably appear most commonly in the addresses. We then proceeded as follows:-

We began with column 18 of the cypher text because we assumed that a frequent address group would be the reason for the "click" in this column. (The "click" in column 24 illustrates that this need not necessarily be the case). We extracted all differences between the cypher texts of messages A to E in this column and obtained these values:-

$$A - B - 4773$$

$$A - C - 3566$$

$$A - DI - 4285$$

$$A - CI$$

$$B - C - 1217$$

$$B - D/E - 2152$$

$$C - D/E - 3369$$

Of each pair of differences (A - B) and (B - A) the smaller difference was always chosen, i.e. that under 5555, as, to save work, only these were included in our difference table.

DECLASSIFIED

Authority E.O. 13526
By SPANARA Date 10/4/11

23.

TOP SECRET

I-51

ENCLOSURE 1

Message A

Please 2530	send 9438	plane 7512	to 1920	(8785	from 6564	Fortr. 1905
Cdr. 5075	Tobruk 5510	to 1920	8th 3022	Army 1037	Q 2215	M 0758
200+ 1177	12 1925	Oct 6315	14th 1501) 0749	evacuate 9945	Lt 9111
spell 6 0006	HA 0801	RV 1822	EY 0525			

Message B

X 1719	machine 1538	out of 0792	action 4809	.6 0000	(8785	Addr. to 8720
Ciph. Off. 9601	8th 3022	Army 1037	from 6564	Ciph. Off. Tobruk 9601	Q 5510	2215
M 0758	/ 1013	300+ 2520	5 4163	16th 4412	Oct 6315) 2097
Send 9438	specialist 4462	for 0097	repair 7102			

Message C

Take 2nd enterpr. 2627	sending 9438	you 1246	Italian 9394	interpret 1177	Capt 4537	spell 8 0008
MA 1301	SS 1919	IG 0907	LI 1209	. 0000	(8785	7th 1928
Armoured 3437	Div. 6720	5 4163	13th 3066	Corps 3205	C 1076	Q 2215
/ 1013	500+ 5406	73 0377	20th 1484) 2097	Please 2530	send 9438
on to 6224	GHQ 5919	Cairo 6726				

Message D

Urgent 7973	request 8529	to 1920	report 7713	effects 8471	new 0904	Arm 4000
. 0000	(8785	Addr. to 8720	13th 3066	Corps 3205	30th 8944	Corps 3205
Australian Force 3732	1665	Australian Base 3732	2065	from 6564	8th 3022	Army 1037
Oct 6315	20th 1484	R 5074	P 2214	/ 1013	33 5046) 0749
Colonel 0358	Spell 9 0009	NE 1405	AT 0120	HE 0805	RB 1802	Y- 2500

DECLASSIFIED

Authority

By

NARA

Date 10/4/11

E.O. 13526

J-51

TOP SECRET

24.

ENCLOSURE 1 (cont)

Message E

Captn. 4537	spell 7 0007	LO 1215	WT 2320	OF 1506	T- 2000	and 0460
Lt. 9111	spell 7 0007	BE 0205	CK 0311	ET 0520	T- 2000	(8785
to 1920	Fortr. 1905	Cdr 5075	HAIFA 5256	from 6564	spell 6 0006	MI 1309
LP 1216	AL 0112	M 0758	EP 2214	87 6388	/ 1013	22 0864
/ 1013	10 1097	Oct 6315	20th 1484). 2097	Will 1276	arrive 8501
HAIFA 5256	by 7299	plane 7512	tomorrow 9782	at 7324	15 3263	00 1538
hours. 9043						

Message F

Germans	take 2nd interpret 2627	preparing 1717	retake 9502	spell 3 0003	BI 0209	R- 1800
spell 4 0004	OM 1513	AR 0118	. 0000	(8785	Adr. to 8720	8th 3022
Army 1037	via 1131	13th 3066	Corps 3205	from 6564	N 8887	Z 0059
Div 6720	E 4329	O 6691	/ 1013	700+ 7575	51 1990	18th 4008
Oct 6315) 0749	request 8529	send 9438	reinforcements 3178		

Message F*

Germans	Take 2nd interpret 3242	preparing 1717	retake 9502	spell 3 0003	BI 0209	R+ 1800
spell 4 0004	OM 1513	AR 0118	. 0000	(8785	Addr. to 8720	8th 3022
Army 1037	via 1131	13th 3066	Corps 3205	from 6564	N 8887	Z 0059
Div 6720	E 4329	O 6691	/ 1013	700+ 7575	51 1990	18th 4008
Oct 6315) 0749	request 8529	send 9438	reinforcements 3178		

DECLASSIFIED

Authority E.O. 13526
 By [Signature] NARA Date 10/4/11

I-51

TOP SECRET

25.

ENCLOSURE 2

	01	02	03	04	05
H A B Q Y :	0 4 6 0 06	0 9 4 3 07	1 2 7 4 08	5 4 8 5 09	2 6 7 5 : 10 :
T O D B A :	3 7 1 9 11	5 1 2 8 12	3 2 6 3 13	5 9 3 1 14	7 3 2 4 : 15 :
R J T K O :	8 2 8 2 16	7 6 1 2 17	6 6 0 3 18	5 2 0 2 19	1 5 3 8 : 20 :
D E L N I :	3 1 7 1 21	3 0 6 7 22	1 9 1 4 23	4 7 1 4 24	1 2 4 3 : 25 :
T A R V E :	5 4 4 0 26	8 5 9 4 27	9 7 8 2 28	0 3 5 8 29	1 0 6 9 : 30 :
K E T T A :	5 6 6 4	8 5 4 9	7 2 9 9	6 3 8 0	7 0 0 3 :
L U D R I :	3 9 7 9	3 7 6 0	4 9 7 8	1 0 6 5	9 4 8 0 :
M A S P A :	2 3 7 5	1 2 7 6	8 5 0 1	0 7 9 6	9 8 5 1 :
Q E P T E :	8 5 0 9	8 5 1 2	1 9 7 6	2 9 4 2	7 0 7 4 :
N I R B I :	1 0 3 6	9 0 4 3	8 3 8 0 :	3 5 3 8	6 1 6 2 :
P O N M O :	8 1 2 7	4 0 3 5	2 4 7 4	4 1 9 7	2 5 8 5 :
S U Q K U :	6 4 2 5	2 6 1 7	5 2 0 5	6 6 1 3	6 9 3 4 :

DECLASSIFIED
 Authority E.O. 13526
 By SP-1 NARA Date 10/4/11

I-51

TOP SECRET

26.

ENCLOSURE 3

Message A)

Book groups:	-	2530	9438	7512	1920	8785	6564	1905	5075
Recypher:	+	<u>3719</u>	<u>5128</u>	<u>3263</u>	<u>5931</u>	<u>7324</u>	<u>8282</u>	<u>7612</u>	<u>6603</u>
Cypher text: TODBA		1289	6790	6751	4011	9649	2728	6717	1638
	-	5510	1920	3022	1037	2215	0758	1177	1925
	+	<u>5202</u>	<u>1538</u>	<u>3171</u>	<u>3067</u>	<u>1914</u>	<u>4714</u>	<u>1243</u>	<u>5440</u>
		0792	0618	0159	2030	9709	4066	0176	4525
	-	6315	1501	0749	9945	9111	0006	0801	1822
	+	<u>8594</u>	<u>9782</u>	<u>0358</u>	<u>1069</u>	<u>5664</u>	<u>8549</u>	<u>7299</u>	<u>6380</u>
		2289	8281	0619	2124	6553	8543	7498	5568
	-	0525							
	+	<u>7003</u>							
		7588	TODBA						

Message F)

Book groups:		3242	2627	1717	9502	0003	0269	1800	0004
Recypher:		<u>3171</u>	<u>3067</u>	<u>1914</u>	<u>4714</u>	<u>1243</u>	<u>5440</u>	<u>8594</u>	<u>9782</u>
Cypher text: DELNI		0939	1440	0207	5212	1240	5241	7794	9788
			10.					15.	
		1513	0118	0000	8785	8720	3022	1037	1131
		<u>0358</u>	<u>1069</u>	<u>5664</u>	<u>8549</u>	<u>7299</u>	<u>6380</u>	<u>7003</u>	<u>3979</u>
		9845	1951	5664	0864	9579	3368	6076	2848
				20.					
		3066	3205	6564	8887	0059	6720	4329	6691
		<u>3760</u>	<u>4978</u>	<u>1065</u>	<u>9480</u>	<u>2375</u>	<u>1276</u>	<u>8501</u>	<u>0796</u>
		0704	1773	5501	1603	2326	5556	4282	4105
			25.					30.	
		1013	7575	1990	4008	6315	0749	8529	9438
		<u>9851</u>	<u>8509</u>	<u>8512</u>	<u>1976</u>	<u>2942</u>	<u>7074</u>	<u>1036</u>	<u>9043</u>
		8848	1034	7622	7978	6637	7335	3517	0615
		3178							
		<u>8380</u>							
		5212	DELNI						

I-51

TOP SECRET

27.

ENCLOSURE 4

Message A)

1289	<u>6790</u>	7651	4011	9649	6717	1638	0792	0618	0159
2030	9709	4066	0176	4525	2289	8281	0619	2124	6553
8543	7498	5568	7588						

Message B)

2000	4590	3571	1132	7324	9992	7002	2280	0501	7617
4466	6404	2509	1595	4437	6074	5629	6946	5754	3677
9111	3837	6393	0901						

Message C)

1192	<u>6790</u>	2027	6647	6257	7614	5302	4393	1631	2972
3067	3239	3896	8816	9720	7674	6726	7153	0093	3459
7536	2893	6013	6629	1982	1230	5540	5841	4571	6659

Message D)

6646	7609	2343	8228	9953	3612	6603	7527	3818	0115
0862	3070	1519	8511	4885	5862	7727	<u>4894</u>	8047	4637
2234	6815	1316	<u>5899</u>	2966	8724	4239	1717	9481	1940
1156	8706	9994	7351						

Message E)

9282	5121	2058	3611	6828	7252	7592	5205	1333	3860
3547	9974	6039	0323	4545	3529	4336	<u>4894</u>	1063	4365
7333	7187	6632	5899	7691	2757	4114	0052	8493	6060
0892	6514	9520	1350	3353	1323	4464	3260	0750	8873
8515	9347								

Message F)

0939	1440	0207	5212	1240	5241	7794	9788	9845	1959
5664	0864	9579	3368	6076	2848	0704	1773	5501	1603
2326	5556	4282	4105	8848	1034	7622	7978	6637	7335
3517	0615	5212							

Recypher:

0358	1069	5664	8549	7299	6380	7003			
------	------	------	------	------	------	------	--	--	--